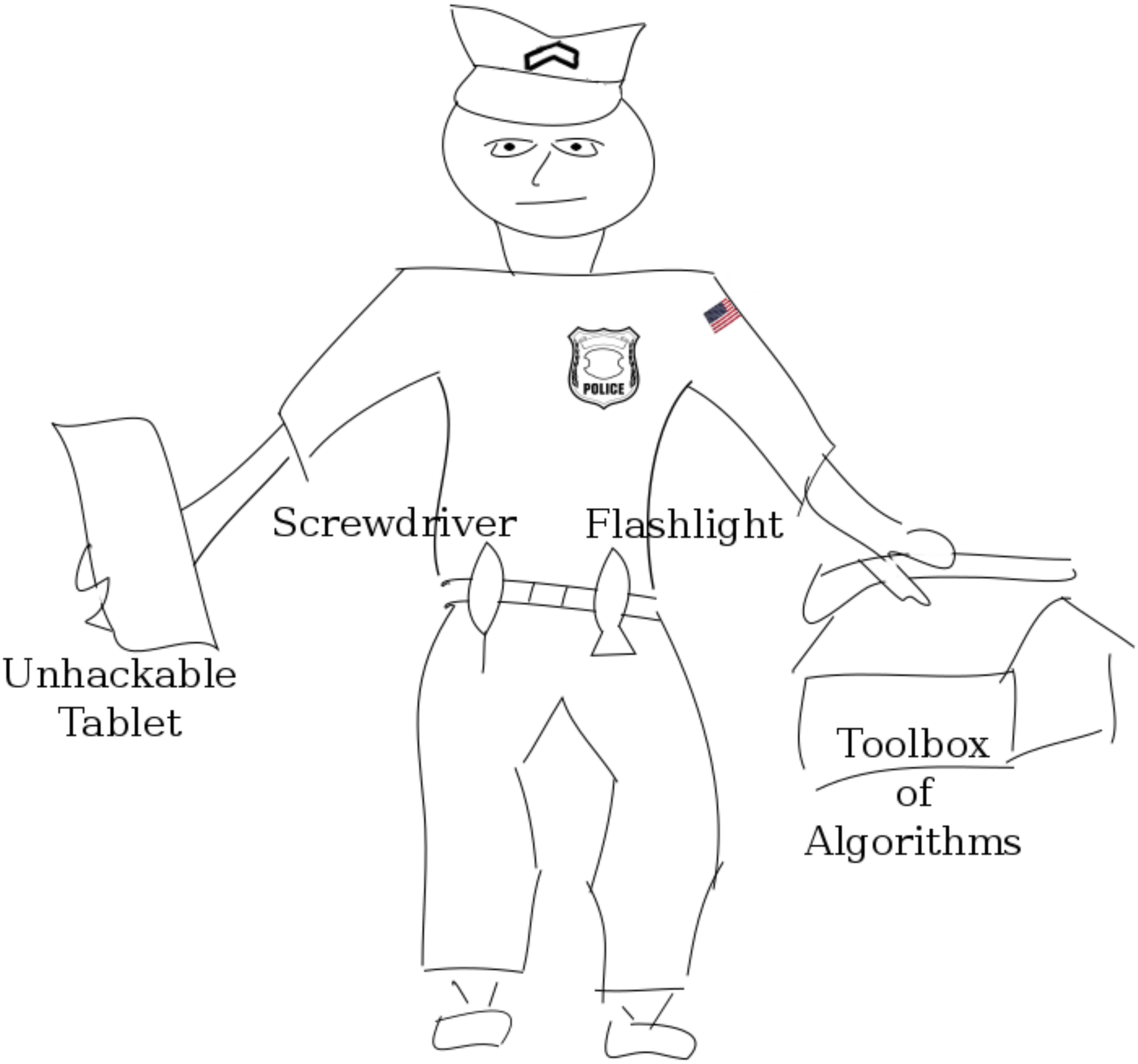
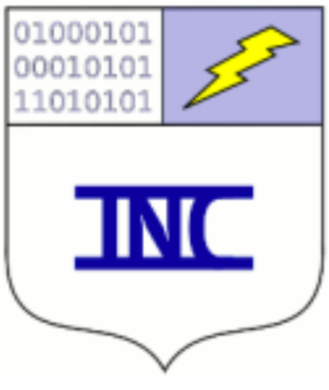
Cyber-Police Officer





To Serve and Protect

Toolbox of Algorithms for use in Jurisdiction

- □ Create Map of Network
- □ Secure a Sub-Network
- □ Authenticate a User by Ownership
- □ Discover Rogue Servers
- □ Locate Rogue Servers

- □ Seize a Rogue Server
- □ Examine Traces of Hacker Activity

Cyber-defenders, such as the FBI, have long used seizure and forensics to track hackers. However, true law-enforcement activities require methods of identifying rogue servers in both cyber and physical space.

Intrepid Net Computing adds five new approaches to the toolbox for cyber-law enforcement. These paradigms are

1. discovering network maps using phylogeny algorithms,
2. securing sub-networks using new DNS algorithms,
3. authenticating users using statistics on knowledge,
4. discovering rogue servers by statistics of DNS, and
5. locating rogue servers using statistics of their ACKs.

Cyber-Police Course Syllabus

Description: A 3-4 unit undergraduate course in advanced methods for policing the Internet. Methods include statistical forensics, *de novo* exploit discovery, distributed systems, and algorithms. Topics will include securing a sub-net, securing an OS, the utility of cryptography, trouble-shooting and debugging. Lectures can be delivered as a 6-week boot-camp.

Pre-requisite: a strong understanding of computer science with the addition of a course in introductory statistics or probability. A computer science bachelor's degree conforming to the ACM standard is appropriate.

Learning Objectives: After the course, a student will be able to serve as a lab-tech for a technology crime lab, will be able to discover evidence according to statistical principles, and will be able to explain those methods to a jury.

Lecture Topics include, but are not limited to:

1. cryptography
2. information theory
3. program verification and theoretical hardness
4. how to know you have been hacked
5. experimental exploit detection
6. detecting exploits with statistical significance
7. buffer over-runs
8. worm life-cycle
9. psychology and HCI of being hacked
10. delta debugging
11. statistical debugging
12. distributed computing
13. networking algorithms
14. exploits used by worms

Contact:
Dr. Brent Kirkpatrick
Intepid Net Computing
Web: www.intrepidnetcomputing.com
Email: bbkirk@intrepidnetcomputing.com
Phone: 406-988-0179
Cell: 406-660-7100